DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

21 February 2019

General Counsel
FOIA Office

MuckRock News
DEPT MR 56753
411A Highland Avenue
Somerville, MA 02144-2516

RE: FOIA 18-168

Dear Sirs/Madams:

This letter responds to your Freedom of Information Act request for a copy of documentation describing the email system used by DISA, including procedures and methods for performing searches of the email system.

There were fifty-six pages responsive your request. Portions of this document have been redacted pursuant to 5 U.S.C. §552 b(7)(E).

Exemption 7E – Applies to information which if released could reasonably be expected to risk circumvention of the law.

If you are not satisfied with this response, you have the right to appeal to the General Counsel, Defense Information Systems Agency, P.O. Box 549, Ft. Meade, MD 20755. Your appeal must be postmarked within 90 days of the date of this response. Both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

For any further assistance and to discuss any aspect of your request, you have the right to contact the Defense Information Systems Agency FOIA Public Liaison at 301-225-6100. Additionally, you have the right to contact the Office of Government Information Services (OGIS) to inquire about the FOIA mediation services they offer. The contact information for OGIS is: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

This concludes the initial determination by this agency. If we can be of further assistance, please do not hesitate to contact Robin M. Berger, FOIA Manager at (301) 225-6104.

Enclosure

ROBERT B. STIRK
Major, USAF
Attorney Advisor

~~Contact DISA OGC prior to releasing this guide outside DoD.~~

FOIA Release Version / Unclassified

DISA

A Combat Support Agency

DISA OFFICE OF THE GENERAL COUNSEL'S DEPARTMENT OF DEFENSE ENTERPRISE EMAIL (DEE) SEARCH GUIDE

Current as of 6 July 2018

Contents

If you have suggestions for improvement, please email

[redacted] (b)(7)(e)

~~Contact DISA-OGC prior to releasing this guide outside DoD.~~

DEE Active Server Search Process

(Journaled NIPR accounts are searched by the Mission Partner's Trusted Agents (TAs); [redacted] is required) (b)(7)(e)

Save time by sending complete documentation (see Guide)

1. Mission Partner defines scope of search (what account(s) to search, what search terms, what time frame, appropriate supporting documentation) and authorizes a Requester/POC to submit the request

DEE emails only

B7E

2. DISA Department of Defense Enterprise Email (DEE) Law Enforcement/Counter Intelligence (LECI) Support Team in-processes all requests and routes within DISA

DISA DEE LECI Support Team will confirm by email

3. DISA OGC confirms documentation sufficient

Search time cannot be estimated

4. Search queued into DEE System

Designated recipient must be government personnel (civilian or military)

5. Search Results uploaded to secure sites

6. Requester emailed instructions for downloading

Requesting organization is solely responsible for release decisions

~~*Contact DISA OGC prior to releasing this guide outside DoD.*~~

-

1. Introduction

This DISA Office of General Counsel (OGC) DEE Search Guide is designed to help Department of Defense (DoD) Enterprise Email (DEE) Mission Partners navigate the process for requesting DEE email searches and get the most out of search results.

This Guide is intended to help non-technical personnel—investigators, attorneys, records professionals, Freedom of Information Act (FOIA) officers, and others—understand how to request searches of the DEE system. This is not a technical document—if you need technical details about the DEE system, please contact your organization's Engagement Executive in DISA's Mission Partner Engagement Office (BDM). (See http://www.disa.mil/Computing/Engagement-Executive .)

This Guide discusses what can be searched, what can't be searched, who can request a search, documentation required, how search results are delivered, and Frequently Asked Questions (FAQ). To make it easier to find the instructions you'll need to make a request, we've organized this version of the Guide by the function of the Requester—FOIA, Investigations, Litigation, NARA Archiving, and Other.

1.1. Legal Status of DoD Enterprise Emails and System

DISA Office of General Counsel (DISA OGC) has determined that DEE emails belong to the DEE Mission Partner provisioning the account—that is the MILDEP, Command, Agency, or other DoD organization paying for a particular user's DEE account—not DISA. DISA is itself a DEE Mission Partner, but we only "own" those emails being generated by accounts that we provision for our own personnel. In other words, DISA has physical custody of the emails residing in DEE, but the DEE Mission Partner still has legal custody.

As currently configured, the DEE system is not a system of records and DISA is **not** the Records Custodian for DoD emails. Email retention and preservation policies are set and executed by DEE Mission Partners, not DISA. Furthermore, DISA neither sets nor enforces acceptable use standards for email use by DEE Mission Partners.

Because DEE emails belong to the Mission Partner, DISA will provide access to emails only to authorized personnel. ***Search warrants, court orders, and subpoenas are not required.*** Any provisioning organization may request a search of its DEE accounts and we will provide the search results according to the process described in this Guide. Investigators with sufficiently documented authority may also request email searches as detailed in this guide.

Please note: For non-DoD organizations, such as FBI or DoJ, we ask that the search request come from the relevant DoD Command or Component. The search request must comply with the requirements discussed below, but if sent by the DoD component will not require a court order or other authority. Also, by having the request run through the Mission Partner, the Mission Partner can search through any journaled accounts covered in the request using their Trusted Agent's b7E in addition to DISA searching the active servers' content. (Please note that DEE active servers hold the regular NIPR and SIPR mailboxes of all users of DEE; journaling is an option for specially designated users, whose inbound/outbound email is copied in its entirety, indexed, and kept for up to ten years. SIPR journaled email is retained in a special mailbox in the active server with normal SIPR email; journaled NIPR email is kept in a separate, dedicated b7E)

When DISA performs a search for DEE emails, we do not review or read the actual emails in the search results. ***DEE Mission Partners, therefore, are responsible for reviewing all search results and making all release determinations.*** This includes release of emails and attachments under discovery orders, FOIA requests, Congressional inquiries, etc.

DISA OGC does not provide legal guidance to DEE Mission Partners. This means that each DoD organization requesting a DEE search must seek legal guidance from its own legal counsel. Each DEE search requester (who we shall refer to as the *Requester/POC*) is responsible for obtaining the legal reviews or approvals required by their Command or Component's chief legal counsel. When in doubt, contact your local legal office for assistance.

1.2. Expectation of Privacy and Information Security

All DoD personnel are given notice, by banners and user agreements, that system use (including the DEE System) is subject to monitoring and, by using DoD systems and equipment, each user consents to monitoring, including use of the DEE System for sending and receiving emails and attachments. ***Individual users have no expectation of privacy when using the DEE system to send or receive messages, including attachments.*** Nevertheless, DEE Mission Partners (provisioning organizations) do have a security interest in the information that their users send or receive through the DEE system.

For non-journaled NIPR or SIPR, and journaled SIPR requests, Mission Partners appoint staff known as "Requester/POC," who are authorized by them to request email searches, serve as DISA's point-of-contact for the request, and receive the results. DISA only provides SIPR email search results to the Requester/POC (and other Government entities with a legitimate requirement) who have documented "need to know" and have authority to request searches

------

and receive results. For NIPR journaled accounts the Mission Partner must designate a Trusted Agent (TA), authorized to access the [redacted] The TA will conduct all searches of journaled accounts provisioned by that Mission Partner. (b)(7)(E)

IMPORTANT: DISA LECI does not search the portions of the journaled NIPR accounts stored in [redacted], only the Mission Partner's Trusted Agents may do that. (b)(7)(E)

DISA understands that contractors provide valuable support to DoD, but as a matter of policy, we will only accept searches from government personnel (military or civilian) and will provide access to search results only to government personnel.

1.3 Definitions:

These definitions apply to this Guide and DEE search requests—they are not meant as technical specifications.

Term	Definition/Comment
B7E Compliance Search Web Console	DISA keeps DEE NIPR journaled accounts in long-term storage in The B7E Search Web Console is the tool used to search journaled accounts. In order to use [redacted] (b)(7)(E)
DEE Service Class	Five classes of Outlook Exchange Mailbox (MBX) service: - Basic - 512 MB Exchange mailbox (OWA only) - Business - 4 GB Exchange mailbox* (Outlook + OWA) - Premium - 10 GB MBX Exchange mailbox* (Outlook + OWA) - Executive - 30 GB MBX Exchange mailbox* (Outlook + OWA) - Senior Executive - 50 GB MBX Exchange mailbox* (Outlook + OWA) * Option to use Journaling for selected mailboxes
DEE Mission Partner	The organization provisioning DEE accounts (e.g., MILDEP HQ, Command, Agency); not to be confused with the "user" (individual).
Department of Defense (DoD) Enterprise Email (DEE) System	DoD's Enterprise Email infrastructure service operated and managed by DISA, includes enterprise-level software and hardware.
Digital signature	Unique identifying information resident on Common Access Card (CAC) and applied to emails, Word documents, .pdf files, etc., to prove identity of sender or signer.

Term	Definition/Comment
DISA DEE LECI Support Team	DISA DEE LECI Support Team, the office within DISA that in-processes all DEE search requests. Their email address is [redacted] (b)(7)(E)
Email	Includes header, subject line, text of message, attachments; "owned" by the DEE Mission Partner, not DISA.
[redacted]	DoD emails. [redacted] To access such emails, contact your component (b)(7)(E)
Enterprise	Federation Constitution-class Cruiser, captained originally by Starfleet Captain Christopher Pike. Also refers to the entire DEE system, as opposed to regional PODs.
Exchange	Microsoft Enterprise-level email software
Expectation of Privacy; **Privacy Interest**	Does not apply to DEE emails—individual users have no right to privacy when sending or receiving emails on the DEE System, even if the emails are going to or from a non-DEE system. Contact your organization's legal counsel for guidance.
Header	Technical term for the top part of every email in the galaxy – it includes the subject and sent/received information that cannot be changed; not usually visible to users, it also contains the metadata of the email message.
Journaling Service **Journaled Account**	An optional service for designated users whose emails may contain official records. Journaling captures and indexes **all** emails sent and received for a period of ten years and secures it in special *journaled mailboxes*. Even if the user deletes a message from his/her Inbox it will still show up in a Trusted Agent's search if it is a journaled account. Because it is more expensive than regular accounts due to the storage requirement, most Mission Partners only use it for General/Flag officers and SES accounts, although other accounts (such as installation commanders) can be journaled. Journaled NIPR email can be searched directly by the Mission Partner's Trusted Agents; journaled SIPR email is searched by DISA upon request by the Mission Partner. Journaled accounts may be used for the CAPSTONE approach to records management of email to comply with the requirements set by the National Archives and Records Administration (NARA). To verify who your component's journaled users are, contact your component's DEE entitlement manager (the person in your organization who manages your organization's DEE accounts), they will be able to tell you if an account is journaled and who the Trusted Agents are. (Contact your component's J-6 or equivalent to find out who your DEE entitlement manager is.)

Term	Definition/Comment
Local drive	A user's laptop or workstation which may contain emails copied from DEE into a .pst file. DISA can't search local drives.
[redacted]	[redacted]
Outlook	The Microsoft client (local machine) software used to read, compose, and manage emails and attachments.
Outlook Web App OWA	Web-based version of Outlook; CAC is required to use and access DEE emails.
POD	PODs are self-contained systems with the technology to deliver DEE services for up to 75K mailboxes. These are located at designated DISA Data Centers.
Preservation	The copying of information from an account and distribution to the requester for them to maintain for as long as they need it. DEE is not a records keeping system, although records are on it.
.pst file	The type of file that Microsoft Outlook uses to store emails and attachments on a local drive. DEE search results are delivered in a .pst file created for each search.
Requester	Referred to as the email Requester/POC, this is the government POC authorized to submit a request for a DEE search (non-journaled NIPR/SIPR email, as well as journaled SIPR email). – this is *not* the same as a FOIA requester.
Search	Querying of DEE System for emails and attachments matching criteria (account, date/time, key words, recipient, etc.) supplied by the Requester.

(b)(7)(E)

Term	Definition/Comment
Trusted Agent (NIPR)	A Mission Partner-designated individual granted the ability to search through journaled NIPR accounts for that Mission Partner. [redacted] his is access to a separate network where the archived journaled NIPR accounts are stored. Once that is granted, they [redacted] The process is detailed in "DEE TTP: Requesting and Conducting a Legal Search of DEE Email, Chapter 4: Conducting a Search (NIPR Only)" at:
Trusted Agent (SIPR)	Mission Partner designated individual authorized to request DISA LECI conduct SIPR searches, including journaled accounts. Typically used by Counter Intelligence and Law Enforcement entities with recurring need to request SIPR searches.
User	DoD personnel who have a DEE account to send/receive emails; the accounts are provisioned by their Mission Partner organization's DEE Entitlement Manager, using the Defense Enterprise Provisioning Online (DEPO) tool.

(b)(7)(e)

(b)(7)(e)

2. Frequently Asked Questions:

Question	Answer
Who can request a search?	Mission Partner "Requester/POC" and Government entities with a legitimate requirement can request a search of non-journaled NIPR/SIPR email and journaled SIPR. (Only a Trusted Agent (someone with added privileges), can perform a direct search of journaled NIPR email; the TA can also be authorized as a Requester/POC if a search of the DEE active servers is requested.
How do I request a search of the active servers?	Send a request to DISA DEE LECI Support. See Section 5 for details.

Question	Answer
How do I request a complete search of the contents of a journaled NIPR account?	A NIPR journaled user has both their normal mailbox in the DEE active servers, and a complete copy of all emails that is kept in another network. [redacted] (b)(7)(E) The journaled account retains everything from the point when the account was created, up to a period of ten years. [redacted] (b)(7)(E) Mission Partners appoint "Trusted Agents" who are given special access to the system where the archives are stored, and can search them without going through DISA. If you believe someone may have a journaled account, you should contact your component's DEE entitlement manager, who can tell you if a particular individual is journaled. (If you do not know who the DEE entitlement manager is in your organization, contact your J-6 or equivalent, they should know).
How do I request a complete search of the contents of a journaled SIPR account?	For SIPR journaled accounts, DISA LECI can search them for you upon request by the Mission Partner Requester/POC. First, confirm the designate individual has a journaled account by contacting your own organization's DEE entitlement manager.
When will my search results be available?	We don't know. It depends on the complexity of the search and the availability of system resources. But, we will contact you as soon as results are ready for download.
How long does it take for a search to be queued into the System?	It depends on the volume of incoming requests. Allow at least 72 hours between the time we get a complete search request and the time a query is keyed into the System.

Question	Answer
How do I get a status of my search request?	If DISA DEE LECI Support Team has confirmed receipt of your request, rest assured that we will let you know when results are available. But, if you need to know the status, send an email to DISA DEE LECI Support Team – be sure to include the DISA Search number.
How will I get the results of my search request?	We will send you a link and instructions to access a secure site.
How do I make a preservation request?	If you need *preservation of an entire account*, please follow the guidelines for Investigations or Litigations. We will then send the entire account contents currently on the active server for you to preserve. If you require legal documentation of the process for actual litigation, contact DISA OGC.
What is a Journaled account?	A journaled account is an optional DEE service that provides Mission Partners the ability to retain all messages and their attachments sent to and from selected journaled mailboxes. While not required for all end-users, it is recommended for high ranking and other designated individuals whose email may contain official records which are subject to legal and regulatory requirements. Messages in journaled accounts are preserved for 10 years. DISA LECI Support Team will not search a Mission Partner's journaled NIPR accounts; this is done by their Trusted Agent as described in "DEE TTP: Requesting and Conducting a Legal Search of DEE Email, Chapter 4: Legal Search of Journaled Email" at: [redacted] (b)(7)(e)
[redacted]	[redacted] (b)(7)(E)
[redacted]?	[redacted] (b)(7)(e)

(b)(7)(E)

Question	Answer
Who decides whether an account is journaled or not?	The provisioning organization makes that determination; journaling can be implemented when an end-user account is set up, or as needed. (journaling is not retroactive, it begins once the journaled account is created). In order to search a NIPR journaled account please see "DEE TTP: Requesting and Conducting a Legal Search of DEE Email, Chapter 4: Conducting a Search (NIPR Only)" at : [redacted]"
Can my organization make all of its user accounts journaled accounts?	Yes, if necessary, but this is rarely done and can be expensive.

(b)(7)(e)

3. Summary of the DEE System

DISA was directed by the DoD Chief Information Officer to build DoD Enterprise Email, a service that provides secure email to the DoD enterprise that is designed to increase operational efficiency and facilitate collaboration across organizational boundaries. As an enterprise-wide service, DEE reduces the cost of operations and maintenance by consolidating hardware into secure, global DISA Data Centers via self-contained units called PODs, where Mission Partner mailboxes are located.

DEE creates a scalable common platform for the DoD (able to support 4.5 million users and 10 million mailboxes for CAC personas and non-person entities), ensuring Agencies can easily and effectively share information among virtual groups that are geographically dispersed and organizationally diverse.

Continuity of Operations: DEE adheres to the Federal Continuity of Operations Plan (COOP) initiative and Disaster Recovery Plan (DRP) requirement. DEE design provides redundancy both locally and remotely for all components of the system, replicating data between paired sites to facilitate continuity of operations/failover in the event of a catastrophic failure.

DEE is implemented at DISA Data Centers throughout the world; POD locations are selected to provide optimal service and performance. These sites are strategically paired to provide failover, with each site having the capacity to support the primary instance and paired site in the event of a failover situation.

B7E virtual private network (VPN) tunnels. This design allows DEE to provide this service with 99.9% availability.

The above discussed capability is for COOP purposes only and does not mean that DISA keeps copies of all emails forever. Each agency is responsible for their own records management practices. DISA does not set record retention policy and procedure for each DoD component or agency. DISA is only responsible for DISA's records management. The DEE is not a system of record, although it contains emails that are records. Each component sets its own records policy in compliance with NARA guidance. The DoD has not set a specific policy for all components, so some are utilizing the NARA CAPSTONE program and saving emails for varying periods of time, depending on the recipient's grade. Others, realizing that only about 10 to 20 percent of all email traffic are really records, are training their employees to sort their own emails and send the ones deserving preservation to a repository.

3.1. Types of DEE Accounts

Currently there are five types of DEE user accounts plus an optional journaling service that can be assigned to any mailbox. DEE Mission Partners determine the type of account for each end-user when the account is provisioned and can change the type using the DEE provisioning portal. The type of account (service class) determines the amount of storage available:

- - Basic - 512 MB Exchange mailbox (OWA only)
- - Business - 4 GB Exchange mailbox* (Outlook + OWA)
- - Premium - 10 GB MBX Exchange mailbox* (Outlook + OWA)
- - Executive - 30 GB MBX Exchange mailbox* (Outlook + OWA)
- - Senior Executive - 50 GB MBX Exchange mailbox* (Outlook + OWA)

* Journaling option available.

NOTE: End-users are responsible for keeping their mailboxes to an optimal size and will receive warnings as they approach their account maximum. Typically, this is when a user will archive the data to their own hard drive or a shared drive.

All classes of DEE mailboxes are accessible for search and hold requests. That said, end-users are able to self-archive and delete email from their mailboxes (this is part of how an optimum mailbox size is maintained). Such mail remains on the DEE servers for up to 14 days, even if "permanently deleted"; email in the 'Deleted Items" folder may be overwritten by DEE after 60 days.

NOTE: While journaled end-users may delete content from their regular DEE mailbox, the journaled mailbox (kept on a separate system) retains ALL email and attachments that were sent and received, beginning once the journaled account begins, for up to ten years. Each provisioning Mission Partner should appoint Trusted Agents to search their own component's journaled NIPR email, following the procedures outlined in the "DEE TTP: Requesting and Conducting a Legal Search of DEE Email." [redacted] to provide Trusted Agents with the ability to search the component's journaled accounts. As noted previously, journaled SIPR email is searched via a request to the DISA LECI Support Team.

(b)(7)(e)

3.2 Deprovisioned Accounts (that are not journaled accounts)

Each email sent or received by a DEE account user exists on the active servers as long as the e-mail is tied to an existing user account and isn't deleted or moved out of the System.

Deprovisioned accounts are accounts that the DEE Mission Partner organization has canceled using the DEE account management portal, or through automatic updates of the CAC system. DEE Mission Partners are advised that when an account is deprovisioned, the System is likely to overwrite the account and all associated data in 120 days. *This means that after 120 days all emails for the deprovisioned/deleted account probably cannot be searched or retrieved by the user or under a DEE search request.*

The way the System handles deleted accounts is subject to change according to DEE policy and storage requirements and limitations. Requesters are advised to submit requests for email searches when needed, regardless of whether the target accounts have been canceled or deleted.

3.3 Deleted Emails (non-Journaled)

There are two ways that an email can be deleted from the DEE System:

- User soft delete: the email will be moved by Outlook from the user's Inbox to the user's Deleted Items folder; the email still exists on the System and can be searched and retrieved for approximately 14 days;

- User hard delete: if the user "hard deletes" the email (empties the Deleted Items folder in Outlook), then the email will remain on the System overnight; it is also retrievable from the "purges" folder for 14 days.

Please remember:

If a user deletes emails, [illegible]
System will use its available space so it will automatically
overwrite any emails to a [illegible] or expired account.

Journaled emails are kept for 10 years, even if the DEE account is deprovisioned.
It is the Mission Partner's responsibility to have a federal records management plan, including transfer of specified data to National Archives and Records Administration.

3.4. Emails Moved to Local Storage

Because all accounts have storage limits on the System, many users will copy emails out of the System into local .pst files. These are files set up by the users or their local technical support and DISA ***cannot*** search them.

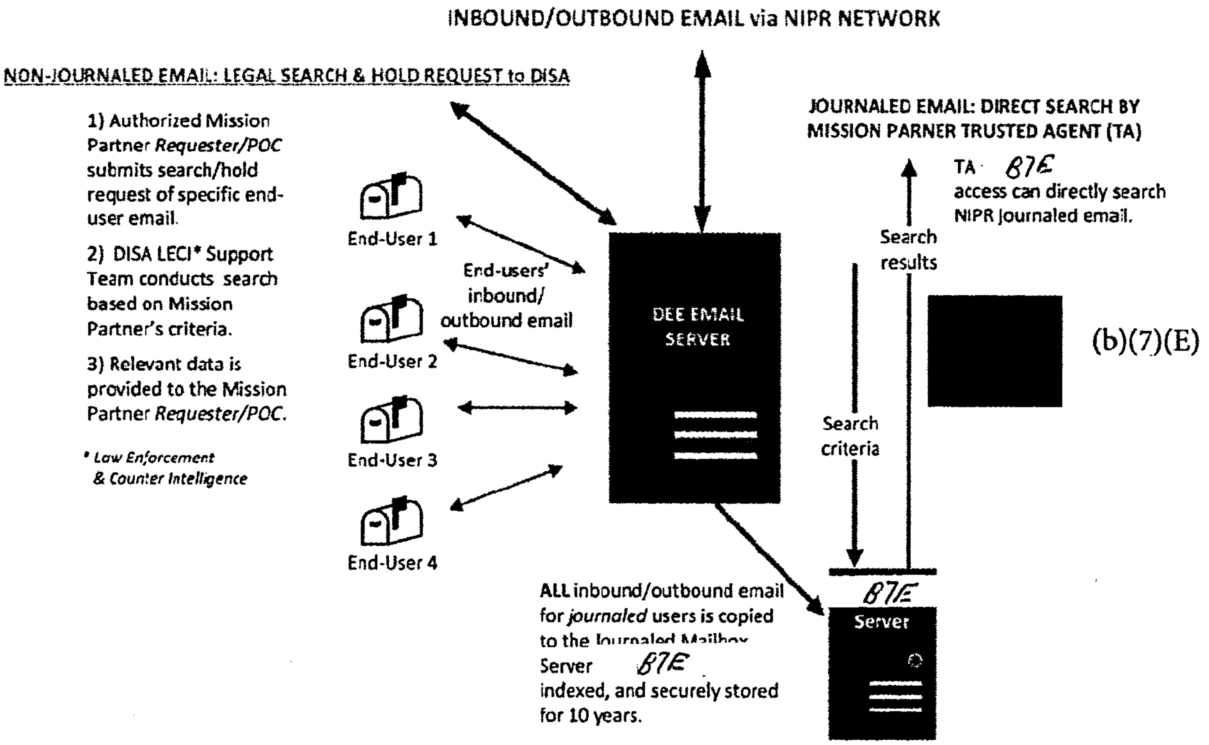
Litigators and investigators should contact their local network or system administrators for assistance in searching local machine drives. Depending on the DEE Mission Partner's internal processes, litigators may also contact their records professionals for assistance.

4. General Information about Searches

4.1 What DISA Can Search for

DISA can search for any emails on the active system from when the Mission Partner began using DEE to the present. We can search any account that ends in B7E For other accounts (for example, emails ending in: B7E , please contact your local network or system administrator for assistance. Journaled accounts are copied onto a separate system, and Mission Partners can search the journaled NIPR mailbox directly through their appointed Trusted Agents.

4.2 Diagram of how NIPR Searches Flow



INBOUND/OUTBOUND EMAIL via NIPR NETWORK

NON-JOURNALED EMAIL: LEGAL SEARCH & HOLD REQUEST to DISA

1) Authorized Mission Partner *Requester/POC* submits search/hold request of specific end-user email.

2) DISA LECI* Support Team conducts search based on Mission Partner's criteria.

3) Relevant data is provided to the Mission Partner *Requester/POC.*

** Law Enforcement & Counter Intelligence*

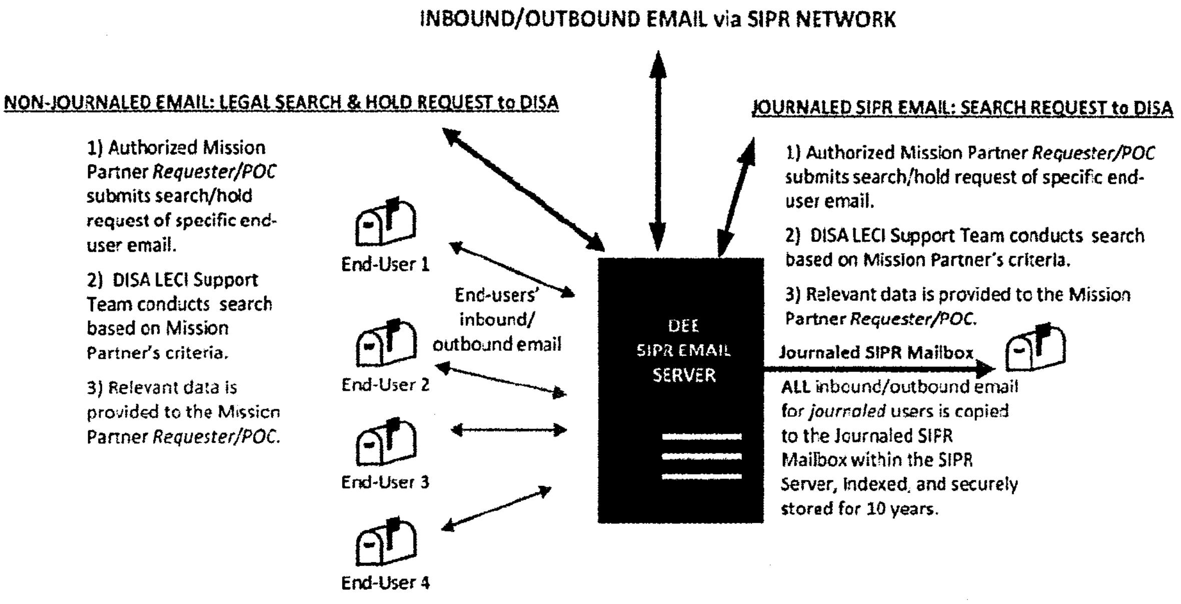
JOURNALED EMAIL: DIRECT SEARCH BY MISSION PARNER TRUSTED AGENT (TA)

TA · b7E access can directly search NIPR journaled email.

[redacted] (b)(7)(E)

ALL inbound/outbound email for *journaled* users is copied to the Journaled Mailbox Server b7E . indexed, and securely stored for 10 years.

4.3 Diagram of How SIPR Searches Flow



INBOUND/OUTBOUND EMAIL via SIPR NETWORK

NON-JOURNALED EMAIL: LEGAL SEARCH & HOLD REQUEST to DISA

1) Authorized Mission Partner *Requester/POC* submits search/hold request of specific end-user email.

2) DISA LECI Support Team conducts search based on Mission Partner's criteria.

3) Relevant data is provided to the Mission Partner *Requester/POC.*

JOURNALED SIPR EMAIL: SEARCH REQUEST to DISA

1) Authorized Mission Partner *Requester/POC* submits search/hold request of specific end-user email.

2) DISA LECI Support Team conducts search based on Mission Partner's criteria.

3) Relevant data is provided to the Mission Partner *Requester/POC.*

ALL inbound/outbound email for *journaled* users is copied to the Journaled SIPR Mailbox within the SIPR Server, indexed, and securely stored for 10 years.

4.4 Each search has three parts: target account(s); date range(s); keyword(s).

4.4.1. Target Accounts

Just because an email address appears in the Global Address Listing (GAL), doesn't mean we can search it. DISA can only search DEE accounts—that means email addresses ending B7E
B7E

DISA cannot look up accounts; they must be provided by the requester (the authorized Mission Partner Trusted Agent or Government entity). A search may be for one or more target accounts. We need the name associated with the account ***and*** we need the email address. For a DEE organizational mailbox or group email box, this is the name of the mailbox and its email address.

Each target account must belong to the requesting organization and fall within the investigative authority of the requesting organization. For example, a request for search of Starfleet Academy target accounts coming from the Klingon High Counsel's FOIA office will be denied—Starfleet Academy owns the accounts and must request the search.

4.4.2. Date Range

Most searches include a date range, which will limit the search results. Because this search process is DEE specific, the date range can be as early as when the end-user's DEE service began; we can't search for emails prior to migration to DEE. Because the DEE System spans many time zones, we use GMT/ZULU by default. If your request is asking for a very narrow date/time range, we recommend you specify GMT/ZULU to ensure accurate results. For best results, consider adding a day on either side of the date range.

A date range is not required, we can search "from account creation to present." A search without a date range will yield more results, so requesters should consider using a date range to narrow the results to reduce the amount of irrelevant data they have to look through.

4.4.3. Keywords or phrases

Keywords and phrases are not required, but search results can be narrowed by including them in the search criteria. Requesters should consider carefully— only emails with exact matches will be in the results.

[redacted] (b)(7)(E)

DISA will not interpret search requests, so any keyword lists should include all acceptable permutations of the keywords or phrases. For example, if you request a search for the "Ferengi Rules of Acquisition", your search results won't capture an email with "Ferengi Rules of Acq." or "the Ferengi Rules." Instead, you should consider requesting "Ferengi" or "Ferengi Rules" or "Rules of Acquisition" as your keywords. DISA can search for one or more terms together but can't search for "but not" (to exclude terms you know you aren't interested in) and also cannot do proximity searches for "X word" within y number of character or words of "Z word." We can search for "tribbles" and "Klingon" within the same email, but we can't specifically search for "tribbles" appearing within ten words of "Klingon."

Requesters can always apply keyword criteria to the search results that the System generates. Search results are delivered in the form of a .pst file set up for the particular request. This means that the requester can search the search results in Outlook. This may be helpful for investigations or broad discovery requests which may require ongoing narrowing of search criteria.

4.5. What We Can't Search for

4.5.1. Transaction or Logging Data

DEE retains log-in data when a user's Outlook logs into the DEE System to upload or download emails, etc. This data relates to the Outlook-DEE System connection, not to the user's local log on. The System does not track when a user logs out because that is done locally, not on the System. The amount of logging data is vast, so it is not retained for more than about 10 days and it is used for System performance measurement, not for auditing user activity.

DISA does not have the hardware or software required to search the logging data collected by the DEE System. If your organization has a compelling need for that data which would justify procurement of the required items and loan to DISA, please contact us to discuss technical requirements and feasibility.

4.5.2. Vague or Undefined Search Criteria

When we get a search request, we design a query that is keyed into the DEE System. DISA cannot interpret requests—if the request isn't specific, we can't design a query and the search is, therefore, delayed.

DISA can't design queries for "including but not limited to" or "related to" keywords. The requester should either list all relevant keyword permutations or leave this part of the search blank. You'll get a larger result (more emails), but you are more likely to get the emails you need.

Likewise, we can't process a search for emails "on or about" a specific date, we need to know the date range.

4.6. Search versus Preservation versus Account Duplication

When DISA processes a request for DEE emails, by default we run a search, meaning we query the System for emails and attachments matching the requested search criteria and the System copies all matching emails into a .pst file set up specifically for the search. This .pst file contains exact copies of the query results, including headers. In the event the request is to preserve an account, we send the entire current contents of the account to the requester for them to preserve.

Occasionally, a law enforcement organization will request that we create a

B7E

documented and approved request of a law enforcement agency. It is not a substitute for a journaled account and will not be maintained indefinitely.

4.7. What Happens When You Request a Search

DISA LECI Support Team personnel receive all incoming search results, log in the requests for tracking purposes, confirms receipt, and sends them to DISA OGC for confirmation that the search documentation is sufficient. No results are sent out until DISA OGC has approved the search.

DISA LECI Support Team personnel will contact the requester if a search request can't be processed or if we encounter any problems. Most often rejections are caused by incomplete documentation or requests for searches of non-DEE target accounts.

Once the query is keyed into the System, the search will continue automatically until all emails matching the search criteria have been located and copied to a .pst file set up for the particular search. When the query completes, DISA LECI Support Team will upload the results (the .pst file) to one of two secured websites (classified or unclassified) and email the Requester with instructions on how to download the results. Once the data is available for download it is the requester's responsibility to download the data **within a 14 day window.** After the 14 days have expired, DISA system administrators will delete the data from our local servers, which means the requester will have to restart the process and face additional delays.

In order to ensure that the search results are not corrupted during the process, we apply ß7E ß7E —any changes to the data in the file will modify the value ß7E This is proof to any court that the data they are viewing was, indeed, the same data sent by DISA.

At no time during the process does DISA examine the emails returned in the search.

[redacted] (b)(7)(E)

[redacted] (b)(7)(E)

[redacted] (b)(7)(E)

[redacted] (b)(7)(E)

[redacted] (b)(7)(E)

5. Search Request Requirements

As discussed above, DEE emails belong to the DEE Mission Partner organization that provisions the account. DISA will make emails held on the active servers available upon request provided that we receive the appropriate documentation.

Please read through the relevant section below and be sure to include the required documentation with your search request. Failure to send the required documentation or incomplete documentation will delay the processing of your request.

Our intent is not to be uncooperative or bureaucratic, but to protect DEE emails and attachments from unauthorized or inappropriate access. When DISA performs a search, we do not look at or read the email results. Email search results may contain classified information, controlled but unclassified information, PII, or privileged information. We need to be sure that whomever we send the search results to is authorized to receive them.

Please remember:

The requesting organization is solely responsible for making release determinations and for ensuring compliance with all information handling laws, regulations, and policies.

5.1. Freedom of Information Act (FOIA) Requests

Each DEE search request in response to a FOIA request must be sent by digitally signed email directly to DISA DEE LECI Support at:

[redacted] (b)(7)(E)

Please remember that DISA cannot estimate when a query will be completed, so FOIA Offices are encouraged to notify FOIA requesters of possible delays in fulfilling requests for emails. FOIA Offices should also be sure to include sufficient time to review the search results for release and/or redaction.

Each search request must include:

- □ DEE target accounts (email addresses), date ranges, and keywords or phrases.
- □ FOIA case number or other file designation.
- □ Confirmation by the FOIA Officer that the target accounts are provisioned by the organization or command making the DEE search request.

redacting or withholding information.

5.2. Investigation Requests

Each DEE search request pursuant to an investigation must be sent via digitally signed email directly to DISA DEE LECI Support at:

[redacted] (b)(7)(E)

Please note that only a small team at DISA has access to these group email boxes. Throughout the DEE search process, we take every reasonable measure to ensure that investigation requests are accessed by the fewest DISA personnel necessary. If your investigation is of an outrageously sensitive nature, please contact either address above and ask to discuss alternate arrangements for submitting a request.

Each search request must include:

- □ DEE target accounts (email addresses), date ranges, and keywords or phrases, as applicable.
- □ Confirmation that the target accounts are provisioned by the same organization conducting the investigation or explanation of the authority of the investigating organization to request the search.
- □ Investigation number or other designation and a brief explanation of the nature of the investigation (e.g., counterintelligence, criminal, court martial, etc.). We don't need to know all the details, just the gist.
- □ Signature by the investigator making the request (digital signature is acceptable) and a Point of Contact to receive the results (usually the same person, but not a contractor).
- □ Appointment memo or other document signed by supervisor, Resident Agent- in-Charge, or other chain of command official stating that the search requester is assigned to the specific investigation and is authorized to request the DEE search and receive the results.
- □ Confirmation by the investigator or supervisor that legal counsel has approved the investigation or is advising the investigator through the course of the investigation and that the request is compliant with all relevant laws, regulations, and policies.

5.2.1. Helpful Hints for Investigation Requests

- The documents required above may be digitally signed emails, .pdf files, or Word files, or a scan of a "wet signature" document.

- Digital signatures must be valid and verifiable.

- DISA will ***not*** accept non-digital electronic signatures such as "//signed."

- Requests will not be processed until all required documentation is received, but DISA will cooperate to preserve as much evidence as possible. Please contact DISA DEE LECI Support if you have a very time-sensitive request.

- Generalized credentials or authorizations are not acceptable—we must have confirmation from your supervisor or chain of command that you are assigned to investigate the particular case.

- ***Your organization is responsible for complying with all relevant laws, regulations, and policies when collecting and using search results in your investigation. Contact your legal counsel for guidance.***

5.3. Litigation or Legal Requests

Each DEE search request pursuant to litigation, a court order, discovery request, etc., must be sent via digitally signed email directly to DISA DEE LECI Support at:

[redacted] (b)(7)(E),

Please remember that DISA cannot estimate when a query will be completed, so litigators are encouraged to obtain necessary extensions or flexible deadlines.

Each search request must include:

□ DEE target accounts (email addresses), date ranges, and keywords or phrases, as applicable.

□ Confirmation that the target accounts are provisioned by the same organization making the search request or explanation of the authority of the litigator to request the search. For cases where it is not appropriate to get approval for the investigation from the provisioning organization (for example, when a criminal investigation involves the commander or IT staff members), we can accept a statement signed by the legal office supporting the investigation in lieu of permission from the provisioning entity.

- ❒ The first page and the signature page from the court order, discovery request, court martial charge, or other relevant filing related to the search request.
- ❒ Signature by the litigator or attorney making the request (digital signature is acceptable) and a Point of Contact to receive the results (usually the same person, but not a contractor).
- ❒ Statement by the litigator or legal counsel that the search request is pursuant to current litigation or is being made in anticipation of litigation.
- ❒ Confirmation by the litigator or legal counsel that the request is compliant with all relevant laws, regulations, and policies.
- ❒ Confirmation by the litigator or legal counsel that the requesting organization is solely responsible for any and all release decisions when using the emails as evidence or in response to a discovery request or court order.

5.3.1. Helpful Hints for Litigation / Investigation Requests

- ➢ The documents required above may be digitally signed emails, .pdf files, or Word files, or a scan of a "wet signature" document.
- ➢ Digital signatures must be valid and verifiable.
- ➢ DISA will ***not*** accept non-digital electronic signatures such as "//signed."
- ➢ Requests will not be processed until all required documentation is received.
- ➢ DISA cannot search local drives, so litigators may need to contact individual users or network administrators for emails stored locally.
- ➢ *Your organization is responsible for complying with all relevant laws, regulations, and policies, including determining whether emails and attachments are releasable under court orders or discovery requests.*

5.4. Third-Party Access Requests

DISA gets periodic requests for access to an individual user's emails because the user has unexpectedly left the Department of Defense, passed away, or is out for an extended period of time. Upon request, DISA will start an Out-of-Office message for the user directing senders to another user or another point of contact.

If a supervisor of an employee needs access to a subordinate's emails, they will need to provide a memorandum from the first O-6 or GS-15 in their chain of command explaining the reason access is needed. For example: "I am CAPT James T. Kirk. LCDR Montgomery Scott, my Chief Engineer, was tragically killed when his shuttle craft crashed into a Dyson Sphere. There is vital engine data stored in his email account which must be processed or the dilithium crystals will explode."

For these searches, the request must be sent by digitally signed email directly to DISA DEE LECI Support at:

[redacted] (b)(7)(E)

Each search request must include:

- □ DEE target account (email address), date ranges, and keywords or phrases.
- □ Description of justification for search (e.g., reason why the employee's email is inaccessible).
- □ Confirmation by the requester that the target accounts are provisioned by the organization or command making the DEE search request.
- □ Government Point of Contact sending the request (can't be contractor).
- □ Designation of recipient who will receive the results.

5.4.1. Helpful Hints for Third-Party Access Requests

- ➢ The documents required above may be digitally signed emails, .pdf files, or Word files, or a scan of a "wet signature" document.

- Digital signatures must be valid and verifiable.
- DISA will ***not*** accept non-digital electronic signatures such as "//signed."
- Requests will not be processed until all required documentation is received.

5.5. Special Requests and NARA Archiving

DISA does not send DEE emails to NARA for archiving, so DEE Mission Partners should request a search for any emails that should be archived. DISA cannot determine which emails need to be archived, but will run specified search term searches of non-journaled NIPR accounts. Because journaled account emails are kept for 10 years after their creation, DISA suggests that Mission Partners have their Trusted Agents archive journaled accounts as needed, certainly before the tenth anniversary of account creation.

In addition, DEE Mission Partners may need to request a search that does not fall into the categories described in Sections 5.1-5.4. For these searches, the request must be sent by digitally signed email directly to DISA DEE LECI Support at:

[redacted] (b)(7)(E)

Each search request must include:

□ DEE target accounts (email addresses), date ranges, and keywords or phrases.

□ Description of purpose of search (e.g., NARA archive).

□ Confirmation by the requester that the target accounts are provisioned by the organization or command making the DEE search request.

□ Government Point of Contact sending the request and receiving the results (can be the FOIA Officer; can't be contractor).

□ If the target accounts belong to a legal counsel office (e.g., OGC attorneys or JAG office), then the requester must confirm that the legal counsel office has been notified of the details of the search request.

□ If the search results may be released or transferred to another DoD organization or outside DoD (other than NARA, because if the information is being sent for staging at NARA, this is not necessary), a signed statement from the Requester's ***chief legal counsel*** acknowledging that:

1. The search results may contain information that is personal, privileged, or otherwise protected from release to the public or outside DoD.
2. The requesting organization (DEE Mission Partner) agrees that it is solely responsible for protecting, withholding and/or redacting all documents produced by the search, including email subjects, texts, and attachments.
3. The requesting organization (DEE Mission Partner) agrees that it is solely responsible for contacting any other organization for clearance to release any information belonging to another organization which is produced by the search.

5.5.1. Helpful Hints for Special Requests

- ➢ The documents required above may be digitally signed emails, .pdf files, or Word files, or a scan of a "wet signature" document.
- ➢ Digital signatures must be valid and verifiable.
- ➢ DISA will ***not*** accept non-digital electronic signatures such as "//signed."
- ➢ Requests will not be processed until all required documentation is received.
- ➢ Remember that DISA will not interpret requests—see Section 4 for more information about search criteria.

➢ ***Your organization is responsible for protecting the search results and making all release decisions, including redacting or withholding information.***

6. Where to Get Help or More Information

If you have questions about submitting a DEE search request, please contact:

[redacted] (b)(7)(E)

~~Contact DISA OGC prior to releasing this guide outside DoD.~~

[redacted] B7E

The office of primary responsibility for this document is the DISA Office of General Counsel in coordination with the DEE Program Management Office. This document is current as of 6 July 2018.

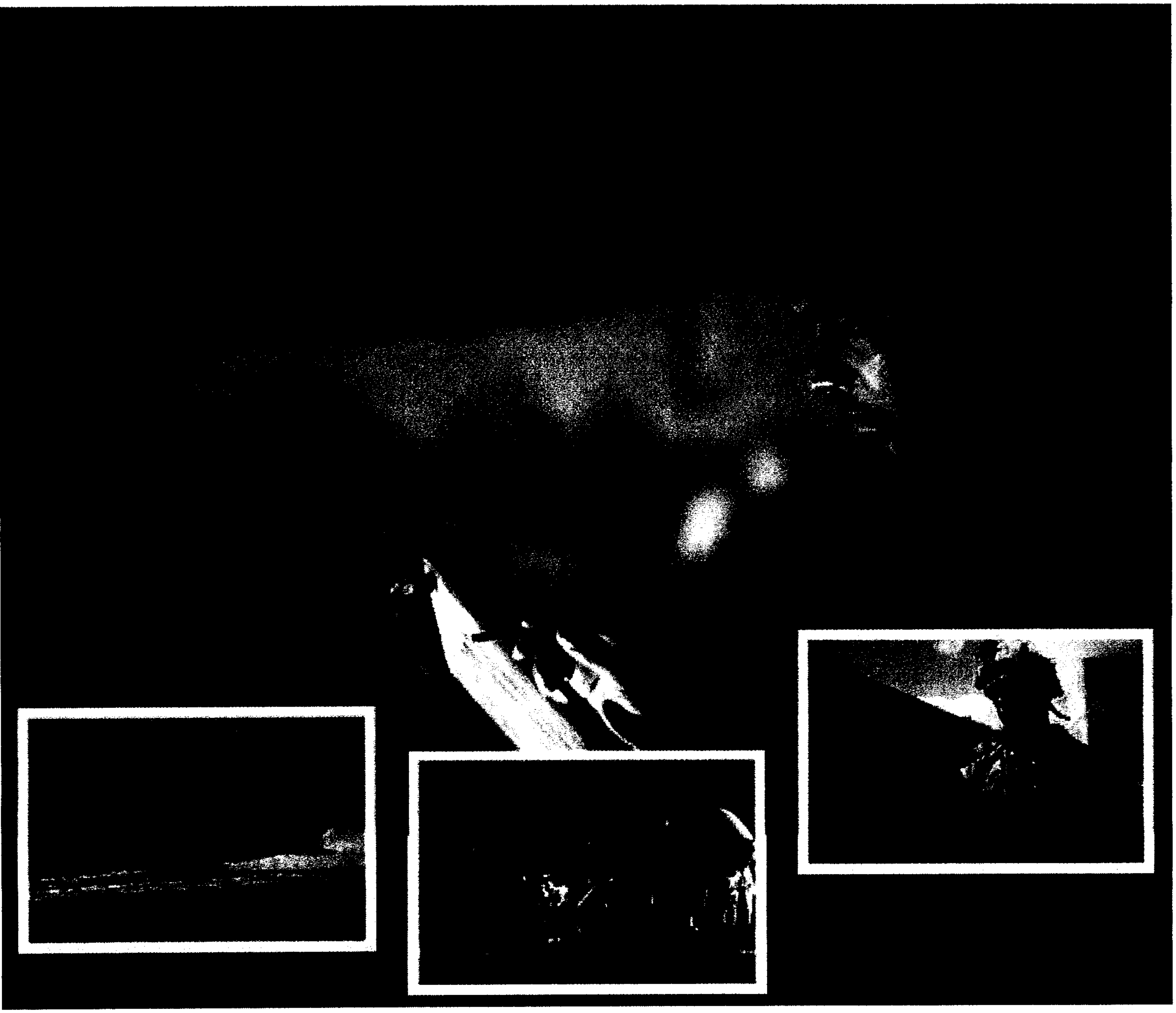
DEFENSE INFORMATION SYSTEMS AGENCY
A COMBAT SUPPORT AGENCY

Department of Defense Enterprise Email (DEE) Tactics, Techniques, and Procedures (TTP):

REQUESTING & CONDUCTING A LEGAL SEARCH AND HOLD OF DEE EMAIL

(TO BE USED IN CONJUNCTION WITH 2018 DISA OGC DEE SEARCH GUIDE)

v1.3 July 16, 2018



Document Approval

(b)(6)

Version	Document Approved By	Date Approved
1.0	[redacted] User Applications Branch (OC / SE34) DOD Enterprise Email (DEE)	November 8, 2016
1.1	[redacted] User Applications Branch (SE34) DOD Enterprise Email (DEE)	June 13, 2017
1.2	[redacted] User Applications Branch (SE34) DOD Enterprise Email (DEE)	June 27, 2017
1.3	[redacted] User Applications Branch (SE34) DOD Enterprise Email (DEE)	July 16, 2018

Revision History

VERSION	DATE	PRIMARY AUTHOR(S)	REVISION/CHANGE	PAGES AFFECTED
1.0 (b)(6)	20161106	DEE Team [redacted]	Original document. This TTP consolidates three separate documents that covered different aspects of the authorized email search process: • *DEE TTP: Overview of the DEE Email Search and Hold Process* • *DEE Guide: Conducting a* B7E B7E *Search* • *DEE Q&A Mission Partner Access to Journaled* B7E	All
1.1	20170613	DEE Team	Updated content to synchronize with the Office of General Counsel 2017 DEE Email Search Guide, Chapters 1-3.	1-7
1.2	20170627	DEE Team	Section 4.1.3: name change - B7E is now called B7E for WIN10.	11
1.3	20180716	DEE Team	Updated to align with 2018 OGC DEE Email Search Guide; clarified descriptions of Request instructions and roles; updated [redacted]ogon steps.	All

(b)(7)(e)

Table of Contents

Tables

Figures

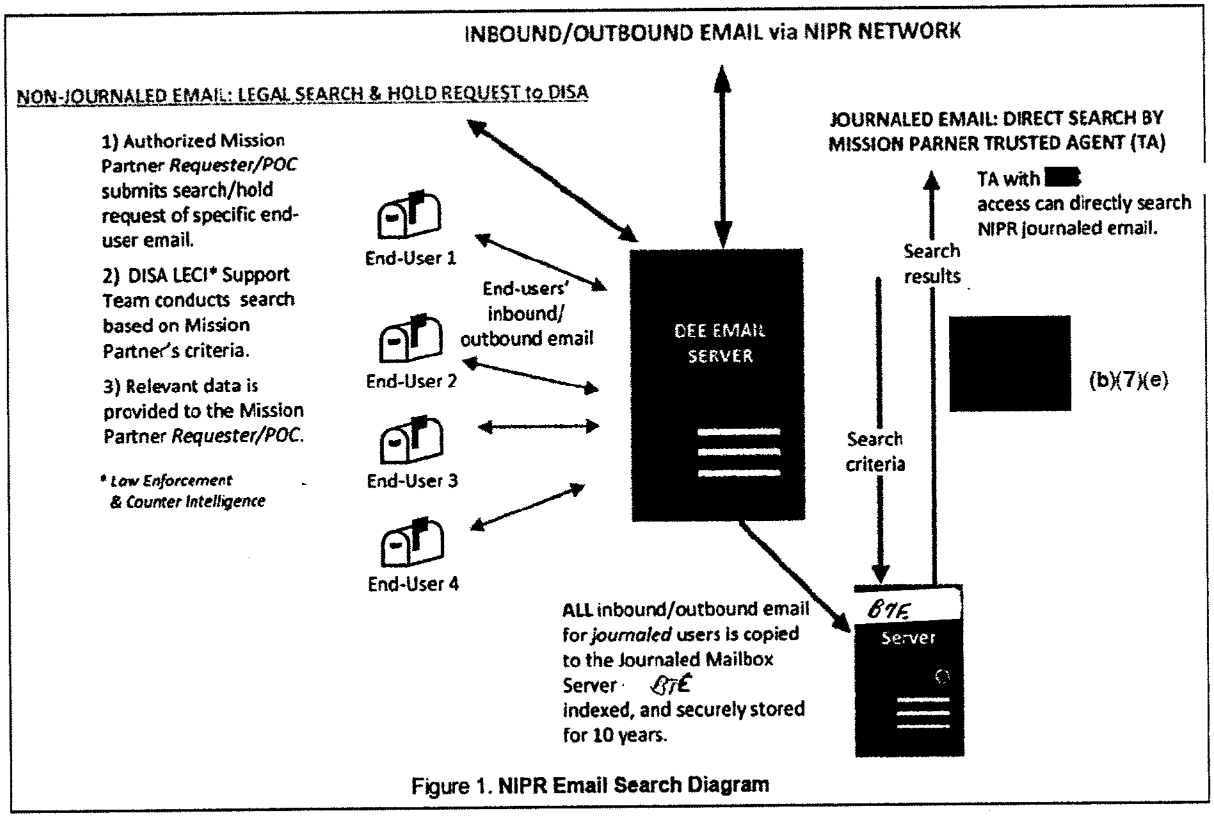
1 Purpose

This TTP provides both a summary of the email search process and practical guidance for Mission Partner organizations; it also touches on Freedom of Information Act requests and transfers of data to the National Archives and Records Administration (NARA). This document is to be used in conjunction with definitive procedures provided by DISA Office of the General Counsel (OGC) and DISA DEE Law Enforcement/Counter Intelligence (LECI) Support in "2018 DISA OGC DEE Search Guide (July 2018)" (t can be downloaded from the DEE Admin SharePoint Library for internal DOD use (for use outside of DOD, please contact OGC): [redacted]). (b)(7)(e)

As the OGC document states (in §1.1),

> *"DISA Office of General Counsel (DISA OGC) has determined that DEE emails belong to the DEE Mission Partner provisioning the account—that is the MILDEP, Command, Agency, or other DOD organization paying for a particular user's DEE account—not DISA. DISA is itself a DEE Mission Partner, but we only "own" those emails being generated by accounts that we provision for our own personnel. In other words, DISA has physical custody of the emails residing in DEE, but the DEE Mission Partner still has legal custody.*
>
> *As currently configured, <u>the DEE system is not a system of records and DISA is **not** the Records Custodian for DOD emails. Email retention and preservation policies are set and executed by DEE Mission Partners, not DISA.</u> Furthermore, DISA neither sets nor enforces acceptable use standards for email use by DEE Mission Partners.*
>
> *Because DEE emails belong to the Mission Partner, DISA will provide access to emails only to authorized personnel. **Search warrants, court orders, and subpoenas are not required.** Any provisioning organization may request a search of its DEE accounts and we will provide the search results according to the process described in this Guide. Investigators with sufficiently documented authority may also request email searches as detailed in this guide."*

As illustrated in figures 1 and 2 on the next page, DEE email is either stored in (a) Exchange servers at DISA Data Centers (and where email of all users is constantly flowing and being selectively deleted by them in the normal course of their work) or (b) in an optional *journaled/NIPR* mailbox (in a SIE) or *journaled/SIPR* mailbox assigned to specified Mission Partner organizations. Journaled mailboxes hold the email of individuals whose messages are considered official records—copies of **all** their sent/received email and attachments are journaled (saved, indexed, searchable, and retrievable by authorized staff) from the beginning of journaling service until ten years after a message was journaled).



NON-JOURNALED EMAIL: LEGAL SEARCH & HOLD REQUEST to DISA

1) Authorized Mission Partner *Requester/POC* submits search/hold request of specific end-user email.

2) DISA LECI* Support Team conducts search based on Mission Partner's criteria.

3) Relevant data is provided to the Mission Partner *Requester/POC.*

** Law Enforcement & Counter Intelligence*

JOURNALED EMAIL: DIRECT SEARCH BY MISSION PARNER TRUSTED AGENT (TA)

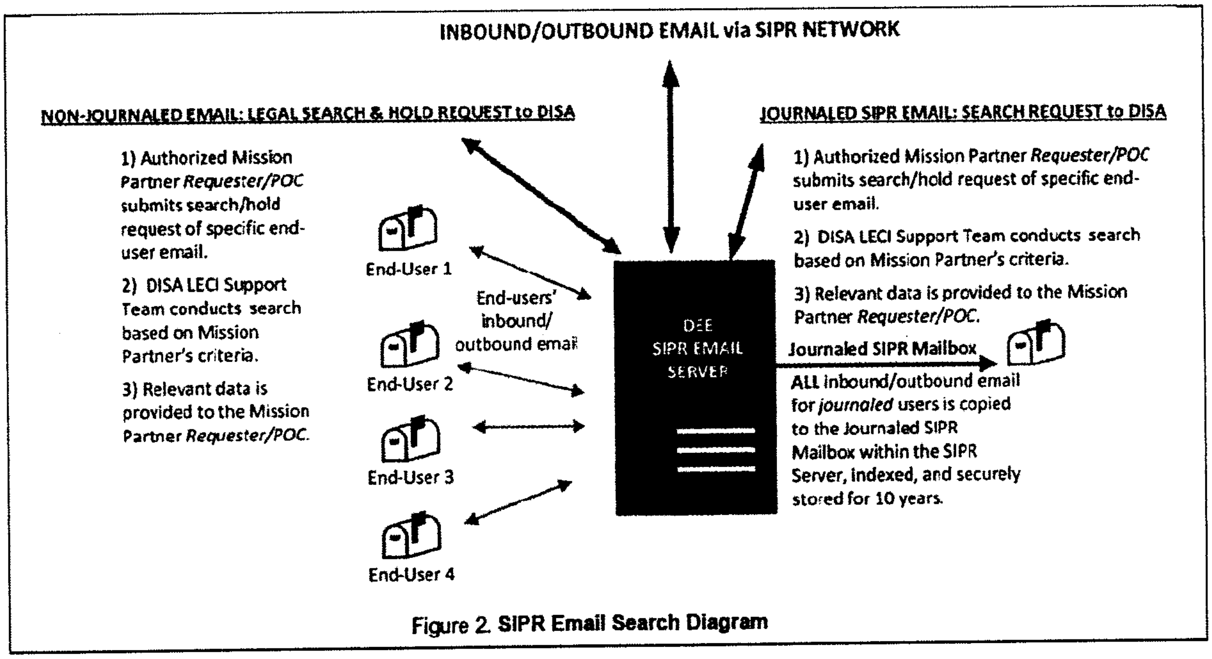
TA with [redacted] access can directly search NIPR journaled email.

(b)(7)(E)

[redacted] (b)(7)(e)

ALL inbound/outbound email for *journaled* users is copied to the Journaled Mailbox Server · B7E indexed, and securely stored for 10 years.

Figure 1. NIPR Email Search Diagram



NON-JOURNALED EMAIL: LEGAL SEARCH & HOLD REQUEST to DISA

1) Authorized Mission Partner *Requester/POC* submits search/hold request of specific end-user email.

2) DISA LECI Support Team conducts search based on Mission Partner's criteria.

3) Relevant data is provided to the Mission Partner *Requester/POC.*

JOURNALED SIPR EMAIL: SEARCH REQUEST to DISA

1) Authorized Mission Partner *Requester/POC* submits search/hold request of specific end-user email.

2) DISA LECI Support Team conducts search based on Mission Partner's criteria.

3) Relevant data is provided to the Mission Partner *Requester/POC.*

ALL inbound/outbound email for *journaled* users is copied to the Journaled SIPR Mailbox within the SIPR Server, indexed, and securely stored for 10 years.

Figure 2. SIPR Email Search Diagram

There are differences in the search process depending on where the email is located:

- Searches of non-journaled/NIPR or SIPR email (see Chapter 2) or journaled/SIPR email (see Chapter 4) require a request to the LECI Support Team from an *email search Requester/POC,* who is authorized by the Mission Partner on a search-by-search basis. The Requester/POC may be part of the Mission Partner's legal team or other office with an authorized need to search and secure a user's email.
- Journaled/NIPR email searches can be conducted directly by properly credentialed Mission Partner Trusted Agents* (no need to request LECI Support); see Chapter 4. The Trusted Agent, like the Requester/POC, usually supports a larger legal team, though neither needs to be a lawyer.

[redacted] (b)(7)(E)

1.1 How this TTP is Organized

- Chapter 2 is an overview of the process for requesting a typical *legal email search and hold* of non-journaled DEE accounts (via LECI Support), whereby DISA will collect, copy, and provide Mission Partners with DEE search results. Please note that Chapter 5 of the **2018 OGC DEE Search Guide** provides the detailed requirements (both search request information and the authorizations) for different types of searches: Freedom of Information Act (FOIA) requests; investigation requests; litigation/legal requests; third-party access requests; and special and NARA archiving requests.
- Chapter 3 provides a brief description of journaled email, of long-term storage, and National Archives and Records Administration (NARA) procedures.
- Chapter 4 covers searches of journaled/NIPR and SIPR email [redacted] (b)(7)(E)

1.2 Intended Audience

This guide is intended for any Mission Partner organization (and its email Requester/POCs, Trusted Agents, and search team members) with a legal requirement and authority to request and perform a search of DEE email.

2 Overview of the Legal Search Process of Non-Journaled Email

NOTE: For Journaled Email searches, proceed to Chapter 3.

2.1 Searching Non-Journaled Users

Legal/statutory searches (also known as litigation or legal searches) of email on NIPR *are initiated by submitting a request (encrypted on NIPR)* to the DISA DEE LECI Support Team at:

DISA DSCC EIS Mailbox Cols-LECI Requests
[redacted] (b)(7)(e)

or

DISA DSCC OPC Mailbox COLS LECI Requests
[redacted] (b)(7)(e)

At a minimum, the following information will be required in order to evaluate the request:

1. Requester/POC's name and contact information
   IMPORTANT: the Requester must be a government employee (not a contractor) and authorized by the Mission Partner.
2. Target mailbox user's name
3. Reason for Request
4. Plus other required authorization information, appointment memo, or other documentation, officially signed, as described in the OGC DEE Search Guide, §5.2 Investigation Requests or §5.3 Litigation or Legal Requests.

Each request will be assigned a tracking number with which related communications (email, etc.) and supporting documentation will be retained by DISA. Emails with sensitive attachments or information must be encrypted.

The requested email will then be held in a special folder that is transferred to the Mission Partner Requester/POC to share with the legal team.

It should be noted that, for any given search, it is possible that not all of the relevant email will be returned in the search results, despite having met the search requirements.

Search results are limited to:

- Emails that currently exist in the user's mailbox
- Unencrypted email
- Encrypted NIPR messages where the search criteria is met (i.e., by sender, receiver, date and/or subject
- Emails that were deleted within 14 days of the start of the legal search

If a user has deleted any emails two weeks prior to the legal search, those emails will not be included in the search results.

Once properly requested data has been compiled by DISA staff, the search results are saved in a newly created mailbox accessible only by the requesting agency or Requester/POC representing the requesting agency.

[redacted] (b)(7)(E)

2.2 SIPR Non-Journaled Email Search

Legal/statutory searches of email on SIPR *are initiated by submitting a request, via SIPRNet,* with a subject line, "Request Search of SIPR Mailboxes," to:

DISA DSCC OPC Mailbox COLS LECI Requests
<[redacted]> , (b)(7)(e)

Include the following information in the body of the message:

1. Requester/POC's name and contact information
2. Target mailbox
3. Reason for request and specific search criteria
4. Plus other required authorization information and documentation as described in the OGC DEE Search Guide.

[redacted] (b)(7)(E)

3 Journaled Mail

Journaling is an optional service provided to Mission Partner organizations (components, etc.). This is recommended for high-ranking and other designated individuals whose email could be considered an official record as defined by each Mission Partner. All journaled NIPR or SIPR email to and from designated user accounts is copied, indexed, and stored in mailboxes that are separate from the user's personal mailbox/es; the journaled email is secure, searchable, and retrievable for authorized purposes, such as a legal search, FOIA request, or transfer to NARA archives. The email cannot be modified or deleted by the user, even if the user has deleted that same email in his or her personal mailbox.

> **NOTE:** Journaling is not retroactive. Once a user is journaled, only new messages *from the date journaling was enabled* will be sent into the journal mailbox. Email that the user sent or received prior will not be included in the journal mailbox.

Once journaled, DISA retains the journaled NIPR or SIPR email on DEE storage servers for a period of ten years. During that time, Mission Partners have the ability to access, search, and copy journaled email into personal storage folders (PST files) via a NIPR or SIPR-specific method:

> **NOTE:** The normal time required for email to be ingested in the journaled/NIPR b7E system is 24 hours, though occasionally that lag time may extend a few days longer due to network circumstances. When beginning a search that includes the most recent email, the TA can ask the b7E Team if any delays will impact the timing of the search.

1) **For NIPR**, the Mission Partner organization is provided an overall journaled mailbox in a DEE b7E storage server that receives the email of all the designated users, that is, the mailbox contains all journaled mail from all users designated within the Mission Partner negotiation. This is searchable only by a Mission Partner Trusted Agent [redacted]; see instructions in §4.6). (b)(7)(e)

> **NOTE:** For additional information on Trusted Agents, [redacted] and the process for conducting journaled email searches please refer to "Chapter 4: Legal Search of Journaled Mail." (b)(7)(E)

2) **For SIPR**, each specified user's inbound/outbound email is copied and secured in an overall journaled/SIPR mailbox in the Mission Partner organization's DEE SIPR server. This is searched by the DISA LECI Support Team upon request, using search parameters provided by the Mission Partner's authorized *email search* Requester/POC. The LECI Support Team will

collect the requested email and provide it to the Mission Partner Requester/POC via a secure .PST file.

[redacted] (b)(7)(E)

3.1 Long-term Storage

Storage of journaled mail for longer than 10 years, in any format, is the responsibility of the Mission Partner and should be stored in accordance with federal records management guidelines and mandates.

Important: DISA retains journaled email on DEE storage servers for a period of ten years. Content older than ten years may be overwritten/deleted and cannot be recovered.

DISA DEE does not provide records management services for maintaining mail outside of the journaled mailbox longer than 10 years.

3.2 National Archives and Records Administration (NARA) Transfer Procedures

Some DEE Mission Partners may have requirements for certain personnel whose email is part of the official record and must be journaled (again, the email to and from designated user accounts is copied and stored in an indexed, secure, searchable, retrievable journal mailbox for future archiving at NARA).

DISA retains journaled email on DEE storage servers for a period of ten years. During that time, Mission Partners have the ability to access, search, and copy journaled email into personal storage folders (PST files):

- As required by DOD and local policy;
- In response to qualified requests; and
- For transfer, periodically, to the NARA collection of “official and permanent records.” This is supposed to happen on a quarterly basis. (Please refer to the OGC DEE Search Guide—sections 3 Summary of the DEE System and 5.5 Special Requests and NARA Archiving—for valuable information.)

Important: Content older than ten years may be overwritten/deleted and cannot be recovered.

Mission Partners are responsible for ensuring required transfers to NARA are made in a timely manner while they have access to the data. After retrieving the .PST files created for them, the Mission Partner can transfer files to NARA using procedures documented on the NARA Email Management portal B7E . The process should be performed each quarter.

When a journaled user leaves the Mission Partner, his or her email does not need to be sent immediately to NARA unless there is a special requirement. The Mission Partner can wait until the next quarter's search is performed. Even after an end- user leaves an organization, their journaled email will still be accessible via the Compliance Search Web Console feature of the DEE journaling solution.

4 Legal Search of Journaled Mail

There are two kinds of journaled email, SIPR and NIPR, and each type is searched in a distinct way.

[redacted]

(b)(7)(E)

4.1 New Journaled Email is Indexed Daily

When preparing to start a search, be aware that while journaled email is archived daily, there is a 24hr lag time before it is searchable in the NIPR b7E Search website (as noted in §3, network issues may cause additional delays).

Once the archive data has been indexed, it is available to be searched from the site. The Columbus-Network Assurance (COLS-NA) team runs content indexing jobs daily, however the indexed data is from the previous day. If the search parameters require present to a past date, the TA should be able to grab everything up to the last 24 hours; or they could wait a day or get assistance accessing the most recent 24hrs.

4.2 Confirming Who is Journaled

Only a select few of a Mission Partner's DEE users have a journaled mailbox. To confirm if someone named in a search is journaled, the Mission Partner's *DEE Entitlement Manager* can use the Defense Enterprise Provisioning Online (DEPO) portal to generate a list of journaled users.

4.3 Journaled SIPR Email Search: Request Required

Because Trusted Agents cannot conduct their own searches in the journaled/SIPR mailbox, there is a slightly different process: the Mission Partner will authorize a Requester/POC for legal search/hold requests that involve those mailboxes.

These actions must be initiated by submitting an encrypted email with a subject line, "Request Search of Journaled SIPR Mailboxes," to:

DISA DSCC OPC Mailbox COLS LECI Requests
<[redacted]> (b)(7)(e)

Include the following information in the body of the message:

1. Requester/POC's name and contact information
2. Target mailbox
3. Reason for request and specific search criteria
4. Plus other required authorization information and documentation as described in the OGC DEE Search Guide.

4.4 Using b7E to Conduct a Compliance Search of Journaled NIPR Email (for Practitioners)

§4.7 provides detailed information on how Mission Partner Trusted Agents access and use the B7E , Compliance Search Web Console (NIPR only) for authorized searches of the journaled mailboxes that reside in B7E

> NOTE: DISA retains journaled email for a period of ten years, during which time Mission Partners have the ability to access, search, and copy email. Mission Partners are responsible for transferring journaled email to the National Archives and Records Administration (NARA) in a timely manner.

4.5 Audience: Mission Partner Trusted Agents

The remainder of this TTP is specifically for Mission Partner Trusted Agents (TAs) who are responsible for performing **NIPR Only** searches of a designated user's journaled email. They support the Mission Partner legal team (or authorized journaled mail recovery effort) as a search agent who keys in the search terms and captures the resulting email.

[redacted] (b)(7)(E)

(b)(7)(E)

[redacted]

(b)(7)(E)

[redacted]

(b)(7)(E)

[redacted]

[redacted]

(b)(7)(E)

4.7 Accessing the Compliance Search Web Console

The Trusted Agent is assigned a unique username and password to use when connecting to the (b)(7)(E) [redacted] This is accomplished by first logging on to a terminal server.

[redacted] (b)(7)(E)

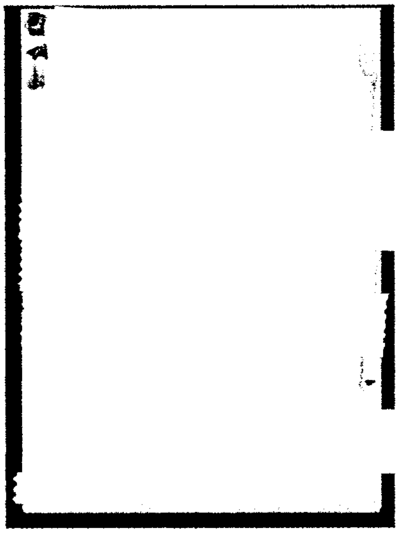
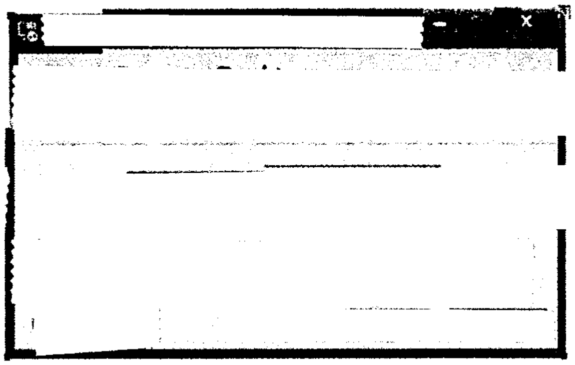


Figure 6. B7E

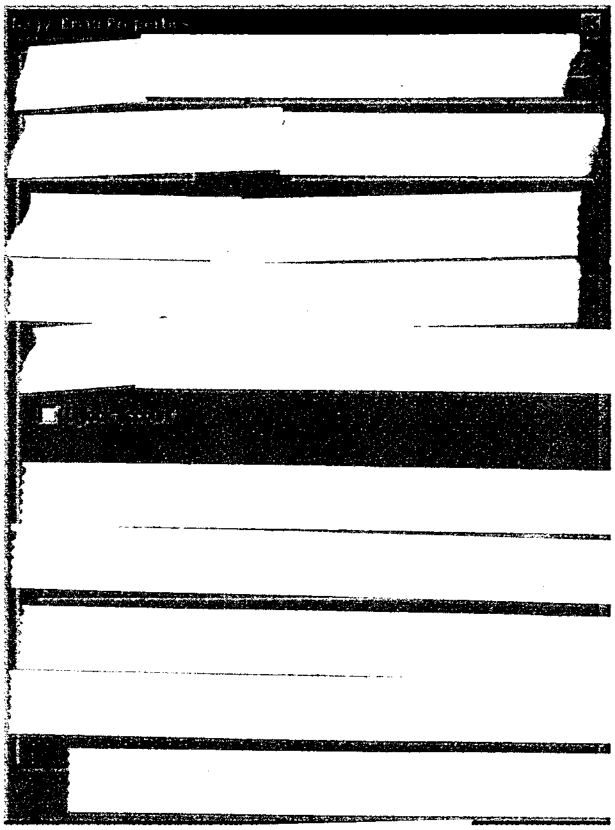
B7E



(b)(7)(e)

Figure 7. B7E

B7E



[redacted]

Figure 8.

4.7.1 Accessing the Web Console

Once the TA has successfully established an [redacted] connection, the Web Console can be accessed. (b)(7)(E)

1. Open a Web browser. In the address field select/enter the appropriate URL from Table 1 for the POD that hosts your organization's journaled mailboxes or click on the link.

Table 1. POD Location URLs

[redacted]

(b)(7)(E)

2. The TA will be prompted to provide

B7

(b)(7)(e) [redacted]

IMPORTANT

B7E

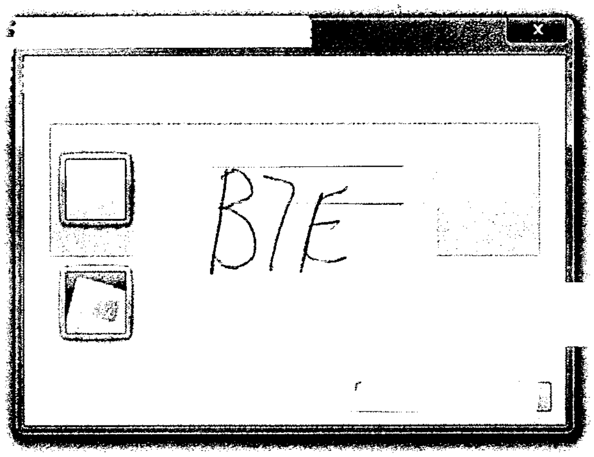
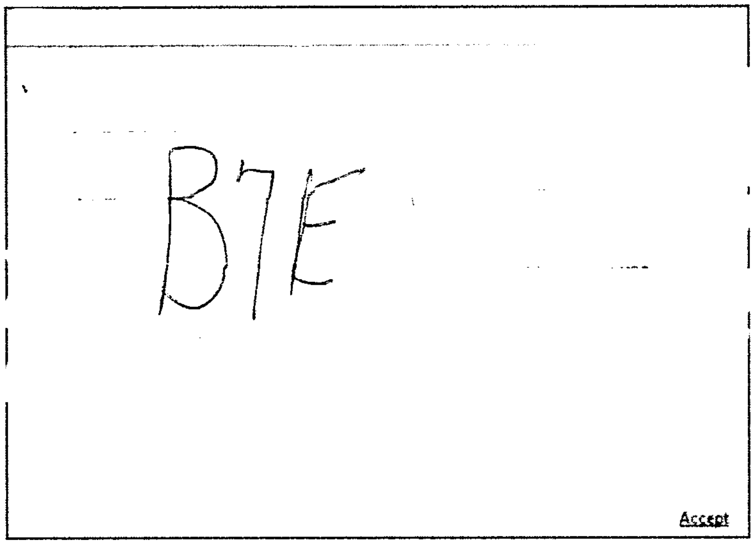


Figure 9. B7E

3. The TA will be prompted B7E

B7E

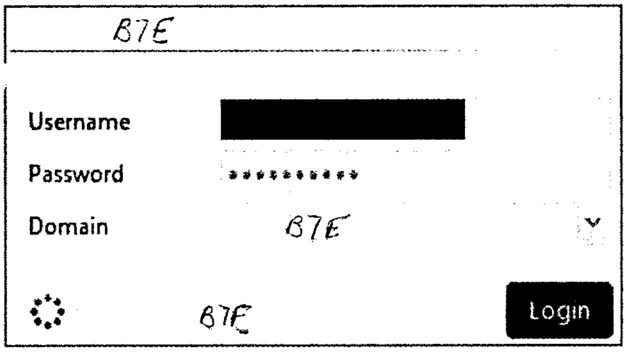
B7E



B7E

Figure 10. B7E

B7E



B7E

Username [redacted]

Password **********

Domain B7E

B7E

Figure 11. **Login Prompt**

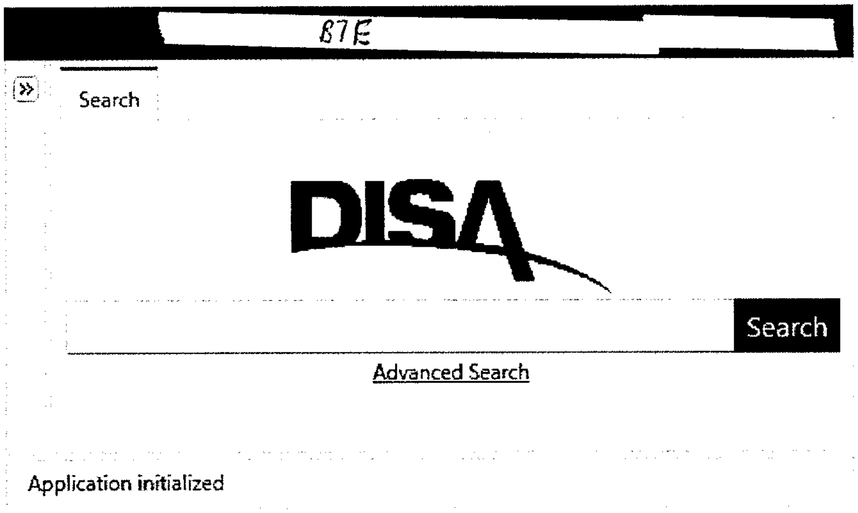
[redacted] (b)(7)(E)

4.8 Using the Compliance Search Web Console

For detailed information on the b7E Content Indexing and Search capability, please reference the following online (b7E

b7E

When the Trusted Agent has successfully logged in, the Compliance Search console will appear (fig. 12).



Application initialized

Figure 12. **Compliance Search Console**

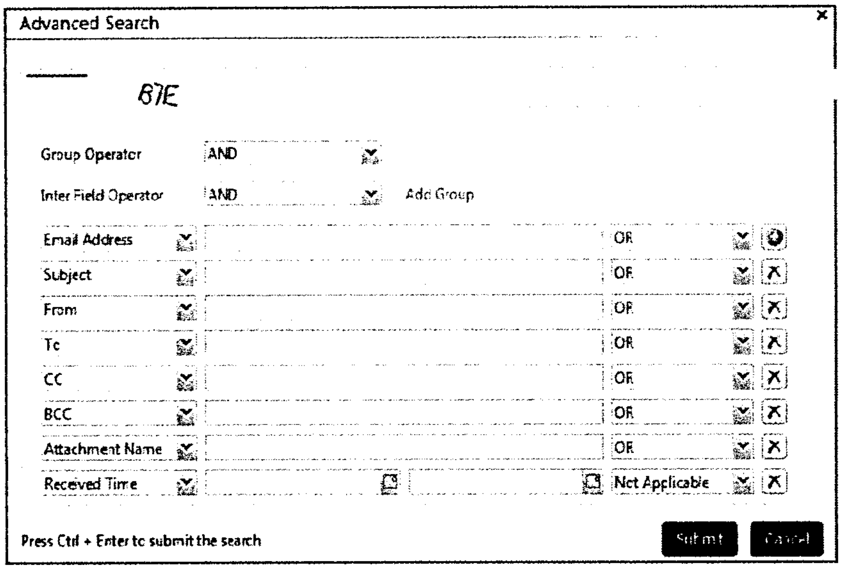
There are two kinds of searches that can be made:

- **A regular search**, which looks for email by entering a keyword or phrase in the search window.
- **An advanced search**, which looks for keywords, email addresses, subject line, and more. The next steps follow the advanced search process. This begins by clicking "Advanced Search."

NOTE: The scope of **Keyword searches** is limited to unencrypted email messages when searching message body and attachments. The other search parameters return results from all archived email.

4.8.1 Conducting an Advanced Search

1. The main **Advanced Search** window appears. There are different fields of criteria to choose from. Fill out the search fields to match the desired criteria and click **Submit**.



Advanced Search

B7E

Group Operator: AND

Inter Field Operator: AND

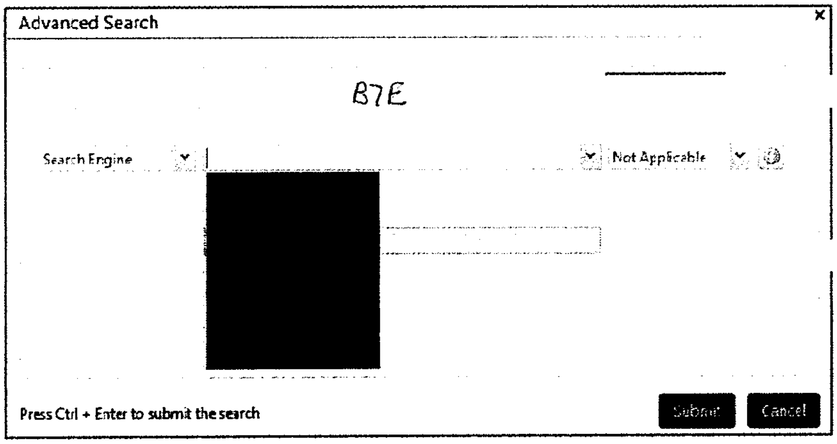
Email Address — OR
Subject — OR
From — OR
To — OR
CC — OR
BCC — OR
Attachment Name — OR
Received Time — Not Applicable

Press Ctrl + Enter to submit the search

Figure 13. **Advance Search**

2. Click on **Search Options**. Choose the appropriate Content Indexing (CI) server. This is the CI server located where the journaling mailbox for your organization is located. If your organization has journaling mailboxes located at various sites, you will be required to conduct a separate search for each site. Click **Submit** to initiate the search query.

NOTE: A TA's CI Server location(s) should have been specified upon the TA's account approval.



Advanced Search

B7E

Search Engine — Not Applicable

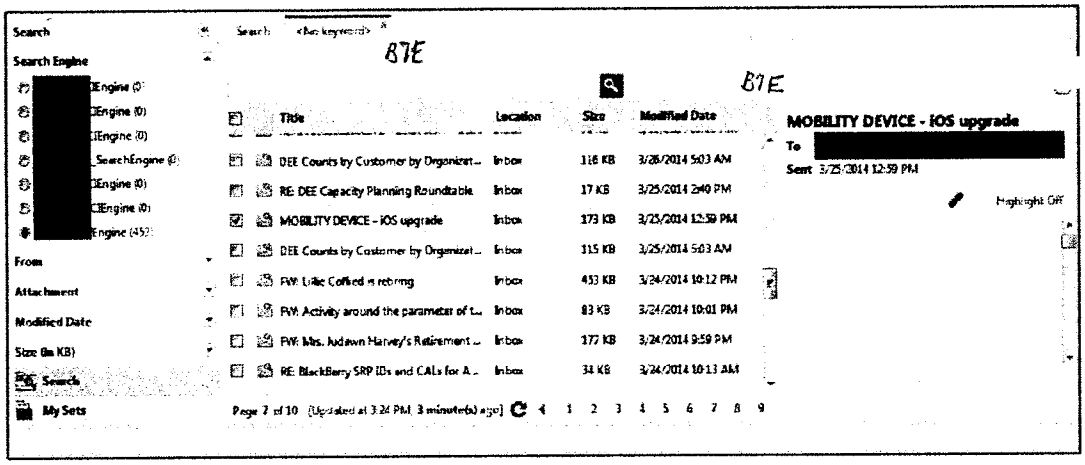
[redacted]

Press Ctrl + Enter to submit the search

(b)(7)(e)

Figure 14. **Advance Search Options**

3. The search query, either using the advanced search if you want a more detailed search, or the basic search function, will run against the chosen search engine. After the query is executed, the results will appear in the window.



Search

Search Engine

[redacted]Engine (0)
Engine (0)
Engine (0)
_SearchEngine (0)
Engine (0)
Engine (0)
Engine (452)

From

Attachment

Modified Date

Size (in KB)

Search

My Sets

Search <No keyword>

B7E

B7E

☐	Title	Location	Size	Modified Date
☐	DEE Counts by Customer by Organizat...	Inbox	116 KB	3/26/2014 5:03 AM
☐	RE: DEE Capacity Planning Roundtable	Inbox	17 KB	3/25/2014 2:40 PM
☑	MOBILITY DEVICE - iOS upgrade	Inbox	173 KB	3/25/2014 12:59 PM
☐	DEE Counts by Customer by Organizat...	Inbox	115 KB	3/25/2014 5:03 AM
☐	FW: Lillie Coffied is retiring	Inbox	453 KB	3/24/2014 10:12 PM
☐	FW: Activity around the parameter of t...	Inbox	83 KB	3/24/2014 10:01 PM
☐	FW: Mrs. Judawn Harvey's Retirement ...	Inbox	177 KB	3/24/2014 9:59 PM
☐	RE: BlackBerry SRP IDs and CALs for A...	Inbox	34 KB	3/24/2014 10:13 AM

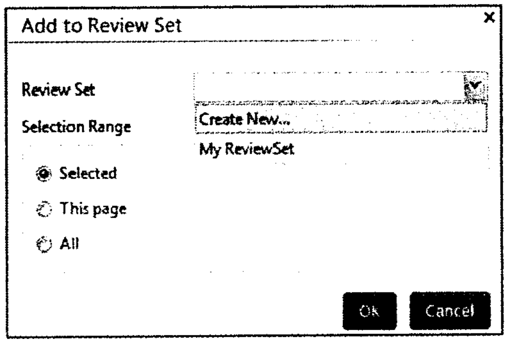
Page 7 of 10 (Updated at 3:24 PM, 3 minute(s) ago) 1 2 3 4 5 6 7 8 9

MOBILITY DEVICE - iOS upgrade
To [redacted]
Sent 3/25/2014 12:59 PM

(b)(7)(e)

Figure 15. **Search Results**

4. You can create a **review set** from the results of the search. Check the "Show" boxes for the results that should be added to the review set and click on **Add to Review Set**. Choose from the list of existing review sets to add the selected range to or create a new review set. If you create a new set, give the set a name and description, then click **OK**. Click **OK** to add the selection range to the review set. A new search results tab with the review set name will appear and be selected after adding the items to the set.

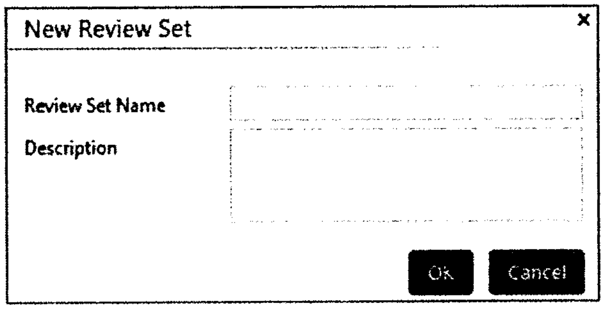


Add to Review Set

Review Set: Create New... / My ReviewSet

Selection Range
● Selected
○ This page
○ All

Figure 16. **Add to Review Set**



New Review Set

Review Set Name

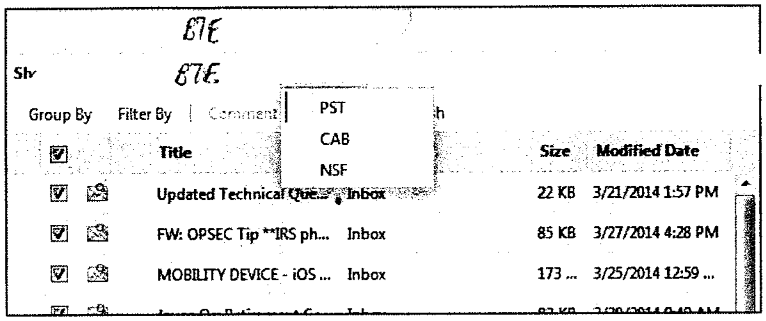
Description

Figure 17. **New Review Set**

The results of a search can be exported in a number of formats for subsequent analysis:

- Personal Storage File (.PST, the common Windows format for archiving Outlook email). Steps 5-7 show how to export results as a .PST.
- Cabinet file (CAB)
- Lotus Notes file (NSF)

5. To export as a PST, check the desired email to export. Click on the **Export To** dropdown and select **PST.**



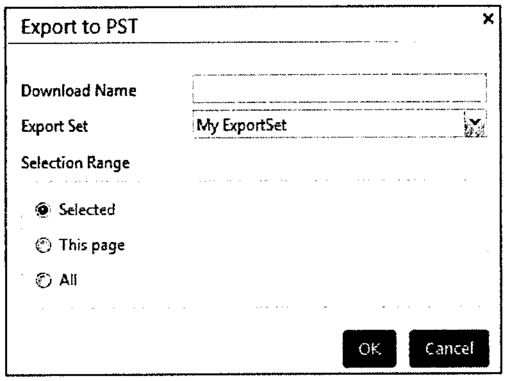
B7E

Slv B7E

☑		Title		Size	Modified Date
☑		Updated Technical Que...	Inbox	22 KB	3/21/2014 1:57 PM
☑		FW: OPSEC Tip **IRS ph...	Inbox	85 KB	3/27/2014 4:28 PM
☑		MOBILITY DEVICE - iOS ...	Inbox	173 ...	3/25/2014 12:59 ...

Figure 18. **Create PST**

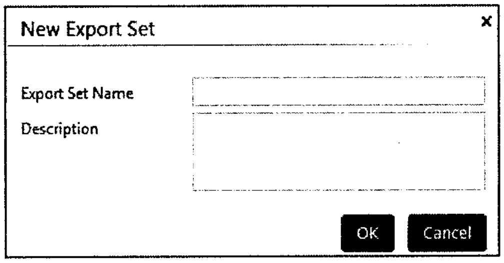
6. Create a download name and choose from the list of existing **export sets** and the selection range to add to the set, or create a new export set. If you create a new set, give the set a name and description, then click **OK** (fig. 19). Click **OK** to add the selection range to the export set (fig. 20).



Export to PST ×

Download Name
Export Set: My ExportSet
Selection Range
● Selected
○ This page
○ All

Figure 19. **Export to PST**

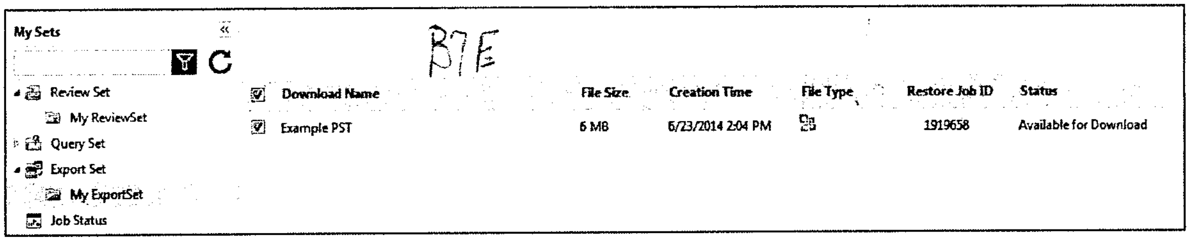


New Export Set ×

Export Set Name
Description

Figure 20. **New Export Set**

7. From the **My Sets** menu on the left, expand **Export Set** and select the export set used in the previous step. Check the download name and click **Download** to save the PST file locally for further use.



B7E

☑	Download Name	File Size	Creation Time	File Type	Restore Job ID	Status
☑	Example PST	6 MB	6/23/2014 2:04 PM		1919658	Available for Download

Figure 21. **Download PST**

Appendix A: Acronyms and Abbreviations

CAB	Cabinet file
CAC	Common Access Card
CI	Content Indexing
DECC	Defense Enterprise Computing Center; now referred to as DISA Data Center.
DISA	Defense Information Systems Agency
DSCC	DISA Defense Supply Center Columbus
EASF	Enterprise Application Service Forest
FQDN	Fully Qualified Domain Name
LECI	Law Enforcement/Counter Intelligence
MECH	Mechanicsburg, Pennsylvania (DISA Data Center)
MONT	Montgomery, Alabama (DISA Data Center)
NIPR	Sensitive but Unclassified Internet Protocol Router Network
NSF	Lotus Notes file
OGC	DISA Office of the General Counsel
OGDN	Ogden (DISA Data Center)
OKC	Oklahoma City (DISA Data Center)
[redacted]	[redacted] (b)(7)(e)
PST	Personal Storage File
PMO	Program Management Office
SAAR	System Authorization Access Request/DD Form 2875
SIPR	Secure Internet Protocol Router Network
STLM	St. Louis, Missouri (DISA Data Center)
TA	Trusted Agent
URL	Uniform Resource Locator
VPN	Virtual Private Network